International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 121 - 126

Intrusion Detection System (IDS) framework for Digital Network

Mr. Ashish K. Uplenchwar, Dr. TanujaDhope
G. H. Raisoni College of Engineering and Management, Wagholi, Pune, India

***Abstract*:** Cyber security has become high priority in Industrial Automation (IA). Here dependable operation is to ensure the security, stability and reliability in power delivery system. Anonymity progress can be easily removed by using the Intrusion Detection System (IDS) framework. In this paper Supervisory Control and Data Acquisition (SCADA)-IDS with protocol based and behavior based analysis is proposed and exemplified in order to detect known and unknown cyber-attacks from inside or outside SCADA systems.This framework provides a hierarchical approach for an integrated security system, comprising distributed IDSs to prevent the anomalous attacks due to access control process.In this article we have compare three methods vizaccess control, protocol base and behavior based whitelist technique. In behavior based there are two techniques used vizlength detector and digital signature.However, for research in the community to progress, such a dataset would be valuable. The proposed system creates new datasets to mitigate vulnerable attacks from cyber-crime side to save the higher level records and system.The simulation result shows thatbehavior based method outperforms the other two methods with respect to time efficiency and accuracy.

Keywords: *Cyber security; intrusion detection; smart grid; supervisory control and data acquisition (SCADA); digital signature technique*

*****

I. INTRODUCTION

Securing the propelled substation environment is just bit of a more broad and critical effort that is obliged to ensure the sheltered operation of front line power systems. There are framework based (NIDS) [1] and host based (HIDS) intrusion acknowledgment structures. A couple of structures might to stop an interference, yet this is not obliged or expected of a checking system. Interference recognizable proof and abhorrence structures (IDPS) are fundamentally focused on recognizing possible scenes, logging information about them, and reporting exercises. Moreover, affiliations use IPsec for various purposes, for instance, recognizing issues with security plans, filing existing risks and keeping individuals from harming security approaches. Framework intrusion acknowledgment structures NIDS [1] are set at a fundamental point or shows inside the framework screen movement to and from all contraptions on the framework. It performs an examination for a passing development all in all subnet, satisfies desires in an unpredictable mode, and matches the action that is gone on the subnets to the library of known ambushes. At the point when the ambush is perceived, or interesting behavior is detected, the alert can be sent to the supervisor.

Instance of the NIDS would be presenting it on the subnet where firewalls are put to check whether some person is endeavoring to break into the firewall. Possibly one would channel all inbound and outbound development, however doing as such might make a bottleneck that would frustrate the general pace of the framework. An IDS which is anomaly based have screen framework development and measure up it against a secured gage. The gage perceive what is "customary" for that framework what sort of exchange velocity is all around used, what traditions are used, what ports and devices generally connect with each other and alert the supervisor or customer when action is gotten which is unpredictable, or in a general sense particular, than the example. The supervisory system might be joined with a data including so as to acquire structure the usage of coded banner over correspondence channels to secure information about the status of the remote rigging for showcase or for recording limits. It is a kind of mechanical control framework (ICS).

Current security countermeasures in SCADA (supervisory control and information procurement) systems dominatingly focus on guaranteeing structures from external intrusions or malignant attacks. Case in point, drawing nearer development to substations, control centers, and corporate frameworks researched by business firewalls or IDS. In any case, this security approach just considers edge protects and ignores internal part area inside a substation framework or a control center. For instance, a planner can enter a substation and partner his or her advanced cell to the neighborhood (LAN). A deliberate or unintended ambush by method for a debased advanced mobile phone now has an upgraded shot of accomplishment in light of the way that edge resistances have been evaded. By and by and in most inconvenient probability circumstances, most of the computerized possessions in SCADA systems ought to be seen as exposed. In any case, we not able to request that every digital resource meet the most imperative security necessities on account of budgetary cost, time and system prerequisites.

Mechanical control systems are machine based structures that screen and control cutting edge techniques that exist in the physical world. Current security countermeasures in SCADA [2] systems predominantly focus on securing structures from outside interferences or pernicious assaults. For example, drawing closer action to substations, control centers, and corporate frameworks audited by business firewalls or IDS. Then again, this security approach just considers outskirt resistances and dismisses inside distinguishing proof inside a substation framework or a control center. There-fore, a draftsman can enter a substation and join his or her versatile PC to the LAN. With the use of IT advancements, new computerized vulnerabilities create in sharp grids and near essential bases. These vulnerabilities could be abused, not only from outside sources, for instance, terrorists, software engineers, contenders, or mechanical observation, moreover from inside threats, for instance, ex-specialists, disappointed agents, pariah dealers, or site engineers. Security for ensuring

the whole brilliant network techno-consistent environment requires the thought of numerous subsystems that make up the savvy matrix, for instance, wide-zone checking insurance and control (WAMPAC), dissemination administration framework (DMS), progressed metering foundation (AMI), and larger amount correspondence architectures at the lattice framework level. The extent of this paper is to concentrate on one essential sub-framework level of the keen matrix environment, particularly digital security for advanced substations.

II. RELATEDWORK

The IDS of this paper is created by simulating so as to utilize information gathered assaults on IEDs and propelling bundle noticing assaults utilizing fashioned location determination convention (ARP) parcels. The revealing capacity of the framework is then tried by mimicking assaults and through honest to goodness client movement. Interruption identification is a powerful countermeasure that is yet to be conveyed in IEC61850 systems [3]. It's prepared to do effectively countering assaults rather than latent hindering as in a firewall. Contrasted with a customary PC organize, the dangers and countermeasures for an IEC61850 system are distinctive. There-fore, the IDS for IEC61850 must be created by utilizing exploratory information based upon mimicked assaults and bundle sniffing [3].

With a specific end goal to enhance the digital security of the savvy framework by using a progressive and conveyed interruption discovery framework in the remote cross section system. Security is enhanced by means of the arrangement of interruption information utilizing the bolster vector machine (SVM) and manufactured resistant framework (AIS) calculations. The viability of the new model for enhancing security is exhibited through various reproductions [3].

To stay away from the digital security dangers, [3] proposes a dispersed interruption recognition framework for shrewd networks (SGDIDS) by creating and conveying a savvy module, the investigating module (AM), in various layers of the brilliant matrix. Different AMs have been inserted at every level of the brilliant lattice - the home territory systems (HANs), neighborhood zone systems (NANs), and wide range systems (WANs), where they had utilized the bolster vector machine (SVM) and simulated safe framework (AIS) to recognize and order malignant information and conceivable digital assaults [3].

An approach for the disclosure of computerized assaults are against mechanical foundations. The key segments of this procedure are the real trick of Critical State, and the assumption that an aggressor going for hurting a mechanical foundation (like a Power Plant) and need to modify for fulfilling that come to fruition the condition of the system from secured to fundamental specific state endorsement, barely material in customary ICT structures, imagines that its general application in the mechanical control field, where the essential states are all things considered surely understood and confined in number. Subsequent to the revelation is engaged around the examination of the system improvement, and not on the dismemberment of the assault headway the IDS for known specific states, can recognize similarly "zero day assaults" [4]. The paper has proposed multi-dimensional metric giving a parametric measure of the partition between a given state and the arrangement of specific states. This metric can be used for taking after the improvement of a system, demonstrating its proximity to the arrangement of predefined particular states [4].

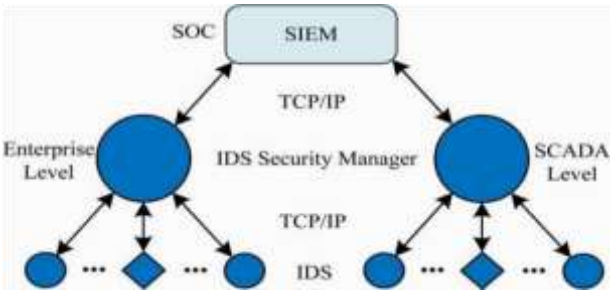

Fig.1 SCADA-IDS security-management system

The principal contribution of this paper [5] is a demonstration that anomaly detection, and specifically methods based on adaptive learning, can provide a useful intrusion detection capability in process control networks. To evaluate two anomaly detection techniques, namely, pattern based detection for communication patterns among hosts, and flow-based detection for traffic patterns for individual flows. These techniques were able to detect some basic attacks launched against the MODBUS servers in our DCS test-bed. Pattern based & flow based anomaly detection has proposed here to improve rate of detection.

III. PROPOSED SYSTEM

Proposing SCADA-IDS structure for recognizing undesirable client on switch, by removing data about access control white rundown, convention based white rundown and conduct base standard from the system. The source and destination IDS are all the significant ascribes going to use in our whole framework. Beneath Architecture demonstrates the framework building design of our SCADA IDS framework. In the given above Architecture there are administrators which are lawful clients and somebody might be assailant. Bundles are trading through LAN system. There are gigantic odds of suspicious parcels assault into the LAN. Interruption identification framework is altered into the system as should be obvious it into the figure. At the point when bundles go into the system Intrusion Detection System begins its working. Our IDS framework is organized of 3 methods.

1. **ACW (Access Control Whitelist):**In this IDS check whitelist of MAC and IP pair which are available in our LAN. In the event that comparing bundle doesn't have MAC-IP pair which has a place with whitelist then it will be identified as assault parcel and which will be put away into Log document for future reference. Generally bundles are not suspicious parcels.

2.**PBW (Protocol Based Whitelist):** If packet belongs to whitelist then protocol based whitelist will check that packet. If corresponding packets matches any of the rule which belongs

to protocol based whitelist then it will be considered as suspicious packet stored into Log file as well as database. Example.

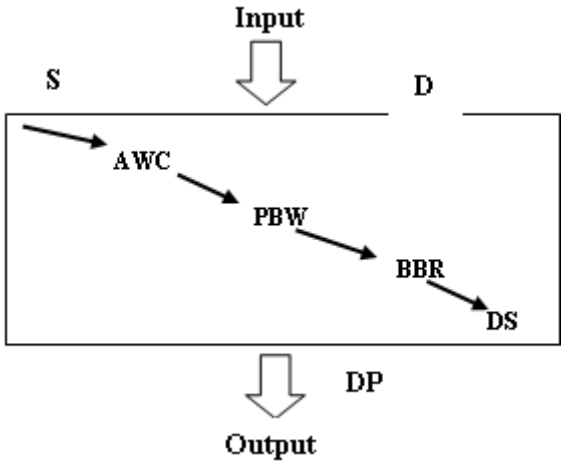

Fig.2 Proposed System Architecture

Rule 1:if(serrr_rate= ("0.00") & login number=("1")& flag("SF")). // this is normal packet
Rule 2:if(flag=("0")) // attack
Rule 3:if(flag=("0") &fail_login1>5) // attack

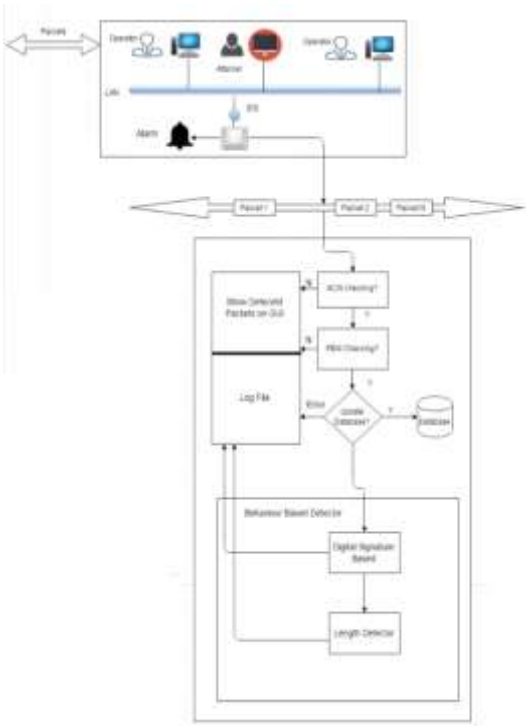

Fig 3. Processes in Detection of Intrusion attacks.

2. BBR (Behavior Based Rule): In this method two techniques are used
Advanced mark era: In this strategy if one administrator needs to send any message to another administrator which is secret then for security reason computerized signature system create keys and signature and sends encoded information towards recipient. At the recipient end mark will be checked and on the off chance that it doesn't coordinate then it is suspicious parcel and put away into the log document. Length indicator: This system checks the genuine payload and length of data bundle on the off chance that it is more noteworthy than payload then parcel is suspicious and will be put away into the log record. At the point when assault found around then IDS will produce caution to think about assault recognition. Thusly entire construction modeling work and we found the bundles are suspicious assault or not.

IV. PROPOSED ALGORITHM

Give S a chance to be the proposed framework which we use to discover the assault location framework through ACW, PBW, BBR and computerized signature era. They furnish our location framework with abilities of precise portrayal for movement practices and identification of known and obscure assaults individually. An advanced mark strategy is produced to upgrade and to accelerate the procedure of SCADA.

As we can see in Fig 3.
S = {D, ACW, PBW, BBW, DP}
Where, S=
System.
D= Dataset.
ACW = Access Control Whitelist.
PBW = Protocol Based Whitelist.
BBW =Behaviour Based Whitelist.
DG= Digital Signature Generation.

Input:
Given an arbitrary dataset X = {x1, x2,….,xn},
Where xi = $[f_1^i, f_2^i, \ldots., f_m^i]T$, $(1 \leq i \leq n)$ represents the ith m-dimensional traffic record.
Where x1, x2,…,xn is n number of packets flowing in the network.

ACW (Access Control Whitelist).
AC = { , $MACdst, IPsrc, IPdst\}$
Where MAC_{src} = Source MAC address.
MAC_{dst} = Destination MAC addresses.
IP_{src} = Source IP address.
IP_{dst}= Destination IP address.

If any of the addresses or ports is not in the corresponding whitelist, the detector will take a predefined action, for example, it will alert in IDS mode and log the detection results. That is

AC $\notin\{AC_{wl}\}\rightarrow$ Actions (alert.log)
Where, AC= , MAC_{dst}, IP_{src} , IP_{dst} and AC_{wl} represent the corresponding whitelist set.

PBW (Protocol Based Whitelist).
Expect there are n bundles originating from dataset as
D={x1, x2, … ., xn},
Where xi = [speaks to the ith m-dimensional movement record.
R = {r1, r2, … . , rn}

Where R is the arrangement of guideline for convention based identification and r1= Rules of whitelist.

On the off chance that when the IDS is sent at the system between two control focuses, the convention based locator just permits correspondence activity agreeing to particular guidelines of convention; else, it will produce a ready message. That is,

P $\{PR\}$ Actions (alert.log)

Where P is the Packet and PR is Protocol based whitelist which contains guidelines of recognizing interruption from compare

BBR(Behavior Based Rules):
Assume there are n packets coming from dataset as
D={x1, x2, · · · ,xn},

Where xi = $[f_1^i, f_2^i, \dots, f_m^i]$T , $(1 \le i \le n)$ represents the ith m-dimensional traffic record.

BBR = {LD, Sig}
Where, BBR is the set of methods for detection of packets belonging to attack packets.

LD=Length Detector
Sig= Signature based Detector.
LD = {P1,P2…Pn}

Where P1,..,Pn are the input packets

When packet contains bytes which indicate the length information about the packet in the payload, it is proposed that a length detector should be applied to detect that whether the number shown in the length bytes is equal to the real length of the payload, such that

$PL_l \neq \rightarrow$ Action (alert, log)

Where $PL_l$is the length value indicated in the length field of the payload, and PL_{rl}stands for the practical length of the payload.

If alert generated then store it into log file.

DG (Digital Signature):

i) Key Generation:
- Choose two vast prime numbers p and q and ascertain n= p x q

- Calculate $\emptyset(n) = (p-1)x\,(q-1)$ and Choose e such that gcd (e, $\emptyset(n)$)=1

- Calculate d such that d X e mod $\emptyset(n)$ = 1
- Choose irregular numbers b and x. Here x ought not relative prime to $\emptyset(n)$ - Calculate c such that bx x c(mod)n=1

- Public key is (n, e, c, x) and private key is (d, b).

ii) Signature Generation:

Figure S1 = (m) mod n if x|s1 (i.e. x is a divisor of s1) then produce s1 once more.

Figure s2 = (H(m) x $bs1$) mod n

H (.) is a restricted hash capacity. (s1, s2) is the mark of message m. Sender sends signature with the message m to beneficiary.

iii) Signature Verification:

Recipient first computes H (m) utilizing the got message m and check the accompanying two conditions for mark confirmation:

Check, if H(m) = mod n
$(m)x \equiv 2x$ x $cs1$ mod n DP (Detected Packets) :

DP={n,m}
Where n is ordinary parcels and M is the pernicious bundles.

(Log File):

Log={x1, x2,..,xn}

Where Log is the arrangement of identified parcels i.e. x1, x2 and so forth.

On the off chance that P ACW or PBW or BBR → $Action\ (Log)$

Where P is the parcel on the off chance that it doesn't has a place with comparing white

V. SIMULATION RESULTS

Identifying aggressors has been principally think about among three calculations, assailants location exactness can be guarantee this parameter. We have characterized the diagram through ascertaining review and exactness values.

$$Recall = \frac{|\{relevant\ document\} \cap \{retrieved\ documents\}|}{|\{relevant\ document\}|}$$

Review in data recovery is the part of the archives that are applicable to the inquiry that are effectively recovered. Exactness is the likelihood that an (arbitrarily chose) recovered record is important. Exactness and review are then characterized as:

$$Precision = \frac{tp}{tp + fp}$$

$$Recall = \frac{tp}{tp + fn}$$

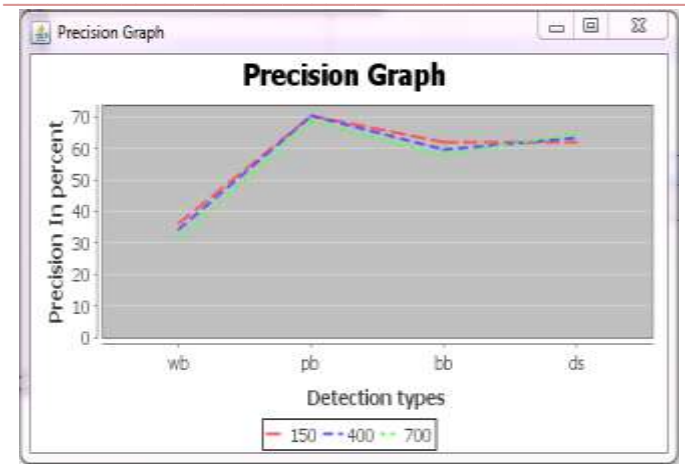

Fig 4. Precision Graph.

Precision				
Dataset	WB	PB	BB	DS
150	41.28	69.72	58.71	65.72
400	38.24	70.47	59.36	66.36
700	38.68	70.47	59.35	66.35

Table 1. Precision Table.

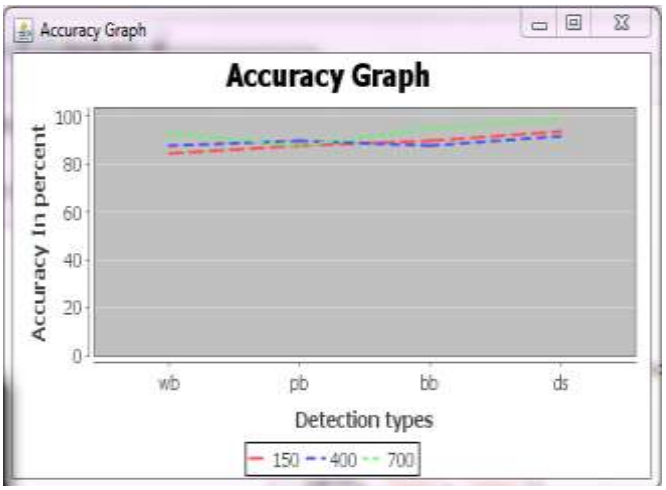

Fig 5. Accuracy Graph.

Accuracy				
Dataset	WB	PB	BB	DS
150	84.9	87.81	98.81	93.81
400	87.96	89.81	87.92	91.92
700	92.97	87.93	94.95	99.87

Table 2. Accuracy Table.

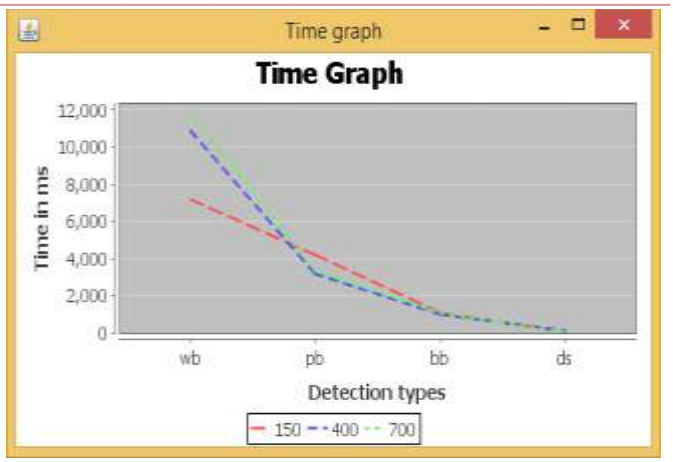

Fig 6. Time graph

Time In ms				
Dataset	WB	PB	BB	DS
150	7210	4225	1028	76
400	10862	3334	1025	146
700	11788	3324	1034	81

Table 3. Time Efficiency Table.

For assessing the execution of whitelists-based (wb), convention based (pb), conduct based (bb) and advanced mark (ds). We have taken the dataset of 150,400 and 700 records .The parameters like exactness, time required for execution and accuracy has been taken into contemplations in mimicking these calculations' execution.

As appeared in above diagrams, Precision of convention and exactness of advanced mark base shows better result as for different procedures for the dataset 700 records and as appeared in time chart computerized signature requires less time to convey for a dataset 150 records.

VI. CONCLUSION

The whitelists-based, convention based and conduct based strategy has been concentrated on and executed the interruption recognition strategies, the conduct based calculation system with computerized signature method is proposed keeping in mind the end goal to screen the whole sensor system. Likewise in light of the Simulation results as appeared in (Fig. and Table) it mirrors that the execution is enhanced as far as precision and time productivity with the assistance of Behavior Based Technique as contrasted and Access Control Whitelist and Protocol Based procedures. Along these lines Digital Signature Technique helps in better checking of cybercrime procedure in systems administration.

REFERENCES

[1] A.A.Ghorbani, W.Lu, and M.Tavallaee, Network Intrusion Detection and Prevention: Concepts and Techniques. 2010, pp. 1–20.

[2] Y. Yang, K. McLaughlin, S. Sezer, ,T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks" IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 29, NO. 3, JUNE 2014, pp. 1092-1102

[3] UpekaKanchanaPremaratne, JagathSamarabandu ,"An Intrusion Detection System for IEC61850 Automated" IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 25, NO. 4, OCTOBER 2010,pp2376-2383

[4] A.Carcano,A. Coletta,M.Guglielmi,M. Masera "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems" IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 2, MAY 2011 ppt 179-186.

[5] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for MODBUSRTU and ASCII industrial control systems,"inProc.,2012,pp.2338–2345

[6] Z. Trabelsi and K. Shuaib, "Man in the middle intrusion detection," in Proc. IEEE Global Telecommun. Conf., 2006, pp. 1–6.

[7] E. D. Knapp, Industrial Network Security: Securing Critical Infra- structure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2011, pp. 60–61.

[8] J. Hurley, A. Munoz, and S. Sezer, "ITACA: Flexible, scalable net- work analysis," in 2012, pp. 1084–1088.

[9] IBM, "IBM security QRadar SIEM," Somers, NY, USA, Tech. rep.WGD03021-USEN-00, Jan. 2013.

[10] Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, Distributed intrusion detection system in a multi-layer network architecture of smartgrids," vol.2,no.4,pp.796–808, Dec. 2011.

[11] M. Crosbie and G. Spafford, "Applying genetic programming to ntrusion detection," presented at the AAAI Fall Symp. Series, AAAI Press, MenloPark, CA, Tech. Rep. FS-95-01, 1995

[12] W. Lu and I. Traore, "Detecting new forms of network intrusion using genetic programming,"Comput. Intell., vol. 20, no. 3, pp. 474–494,2004.

[13] "Communication Pattern Anomaly Detection In Process Control Systems" Alfonso Valdes, Steven Cheung 22 - 29 11-12 May 2009 978-1-4244-4178-5

[14] P. Gross, J. Parekh, and G. Kaiser, "Secure selecticast for collaborative intrusion detection systems," inProc. Int. Workshop on DEBS, 2004

[15] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Q. Yao, B.Pranggono, and H. F. Wang, "Man-in-the-middle attack testbedinves-tigating cyber-security vulnerabilities in smart grid SCADA systems,"inProc. IET Int. Conf. Sustain. Power Gen. Supply, 2012, pp. 1–8.

[16] IEEE Standard Communication Delivery Time Performance Require-ments for Electric Power Substation Automation, IEEE Standard 1646–2004, Feb. 2005.

[17] De Ocampo, Frances Bernadette C, Del Castillo, Trisha Mari L Gomez, Miguel Alberto N "AUTOMATED SIGNATURE CREATOR FOR A SIGNATURE BASED INTRUSION DETECTION SYSTEM WITH NETWORK ATTACK DETECTION CAPABILITIES (PANCAKES)" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(1): 25-35 , 2013 (ISSN: 2305-0012)

[18] Huang Lu, Jie Li, and Hisao Kameda "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature"This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceeding.

AUTHORS

Mr. Ashish K. Uplenchwaris a P. G. Scholar in the Computer Engineering Department, G. H. Raisoni College of Engineering and Management, Wagholi, Pune. He has received Bachelor of Technology degree (BTech) in Computer Science and Engineering in 2012 from MIT, Aurangabad, India. His research interests are Wireless Networks, Computer Networks, Database management etc.

Dr.TanujaSatishDhope (Shendkar) is a full time Associate Professor at Department of Computer ,G.H.Raisoni College of engineering, Pune India. She has acquired her Ph.D in wireless communication at University of Zagreb, Croatia under Erasmus Mundus Mobility for Life Project in 2012. She graduated in Electronics and Telecommunication engineering at Cummins College of Engineering, University of Pune in 1999. She has received Master in Electronics Engineering from Walchand college of Engineering, Sangli, Shivaji University in 2007. Her research focus is on cognitive radio network optimization with spectrum sensing algorithms, radio channel modelling for cognitive radio, wireless sensor network, cooperative spectrum sensing, Direction of arrival (DoA) Estimation algorithms in Cognitive Radio and in SDMA. She published 24 scientific papers in journals and conference proceedings. She has reviewed 7 IEEE conference papers and honoured as 'Session Chair' at ICACCI 2013 conference in Mysore.